UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	**Case No. 4:22-cr-612**
	§	
CONSTANTINESCU, *et al.*	§	**The Honorable Andrew S. Hanen**
	§	
Defendants.	§	

United States' Response in Opposition to Defendants' Motion to Suppress

The United States, by and through its undersigned counsel, responds to Defendants' Motion to Suppress, ECF No. 451 ("Motion"). The Motion is without legal merit and defied by the factual record. The Court should deny it.

I. Introduction

The Motion is yet another example of Defendants' efforts to muddy the record in this case with groundless factual assertions and faulty legal arguments. No basis exists for Defendants' request for "blanket suppression" of the evidence obtained from Twitter, Inc. ("Twitter") (now called "X") and Discord, Inc. ("Discord"), two third-party social media providers.

Stripped of its empty invective, Defendants' Motion boils down to:

(1) (erroneously) alleged technical arguments regarding search warrants under Rule 41 of the Federal Rules of Criminal Procedure; and

(2) complaints that the United States was willing to produce to Defendants—in a good faith *response* to Defendant Hennessey's repeated demands—a broader range of digital files than the United States has actually reviewed and has used (or will use) to prosecute this case.

These arguments fail because the United States executed valid warrants that were based on probable cause and properly issued by Magistrate Judges in this District. The United States diligently obtained the information ordered for disclosure by those warrants, and then carefully scoped its review and seizure of relevant records to the confines set out in the warrants. Each step was taken in good faith, and nothing outside the scope of the warrant will be used against Defendants at trial. Defendants are not entitled to any relief, much less the extreme relief of "blanket suppression" of all records from Twitter and Discord that they urge on the Court. (*See* ECF No. 451 at 23.)

II. Background

As part of its investigation in this case, the United States applied for search warrants to be executed on Twitter and Discord. The warrants sought the search and seizure of business records, subscriber information, communications content, and other information associated with Defendants' activity on the platforms ("Twitter Warrant," "Discord Warrant" or "Social-Media Warrants"). (*See* ECF No. 451, Exs. E, F.) These warrant applications, submitted under the Stored Communications Act, 18 U.S.C. § 2703, were supported by affidavits and accompanied by attachments specifying the property to be searched (Attachment A) (*i.e.*, the social media accounts and servers at Twitter and Discord) and the particular things to be seized (Attachment B).

Attachment B was divided into two parts:

1. Step 1 ordered Twitter or Discord to disclose certain information, comprising a broad range of account information, content, and metadata; and

2. Step 2 authorized the United States to search that information and seize a subset of it, which comprised a narrower set of categories relevant to the elements of the offenses under investigation.

The Social-Media Warrants provided that "review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts." (ECF No. 451, Exs. E, F at 49.) Further, the Warrants authorized the FBI to "deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review." (*Id.* at 50.) The Warrants did not impose a time limitation for the review or retention of the electronic data. *See generally id.*

The Social-Media Warrants were authorized by Magistrate Judges of this Court in August and September of 2022, respectively, and were promptly executed by being served on Twitter and Discord within 14 days of issuance.

After receipt of information from Twitter and Discord under the Social-Media Warrants, the United States promptly commenced a review of the materials provided in accordance with the procedure articulated in Attachment B. To assist in that review and as permitted by the Social-Media Warrants, the United States used a digital analyst, Joseph Varani, to help process the Twitter and Discord records. Mr. Varani ran programming scripts to, for example, render the content readable, remove duplicate records, and ran search terms to identify materials to be seized, consistent with Attachment B's procedures.

Based on its review, the United States maintained for its case file a limited subset of the information produced under the Social Media Warrants and stopped its review of any information not contained in that subset (the "Case File Return"). The information in the Case File Return included, among other things, (1) direct messages (*i.e.*, one-on-one messages) from both Twitter and Discord that involved at least one Defendant and had "hits" on a defined set of search terms, which were provided to Defendants in discovery; (2) group messages (conversations among two

or more participants, involving at least one Defendant) from both Twitter and Discord that similarly had hits on the same set of search terms; (3) the Defendants' public tweets for the relevant period; (4) several public "servers" (*i.e.*, public chatrooms or "floors") from Discord; and (5) certain subscriber data (*e.g.*, follower counts and identifying information associated with each account). The Case File Return also included "processed" messages that connected a relevant message to any media, such as a picture or a video, associated with it.

Of note, the contents of the Case File Return were finalized before the return of the Indictment on December 7, 2022. Information disclosed by Twitter or Discord but not responsive to these parameters was not reviewed or seized for the United States' case file.

The United States then produced the Case File Return to Defendants as part of its initial discovery productions in this case. Also as permitted by the warrants, the United States maintained a complete original copy of the records disclosed by Twitter and Discord for evidentiary integrity, separated from the United States' Case File Return.

In and around March 2023 and in the course of preparing for trial, the United States observed that certain information, particularly media files associated with certain Tweets and internet protocol ("IP") address data for one user account, was missing from Twitter's initial disclosure in response to the Twitter Warrant.[1] This information was clearly within the scope of the Twitter Warrant, as issued, but had been omitted—apparently inadvertently—by Twitter in its initial disclosure. Accordingly, an attorney for the United States contacted Twitter in March 2023 and April 2023 to request the media files and later the IP address data for Defendant

[1] As noted above, certain of the "processed" messages from Twitter were missing associated media for a range of tweets for several of the at-issue Twitter accounts. The United States, with the assistance of Mr. Varani, concluded that the at-issue media files were never produced by Twitter pursuant to the Twitter Warrant.

Constantinescu, respectively. Twitter produced the responsive information citing to the original Social-Media Warrants without requiring additional legal process. (*See, e.g.*, ECF No. 451, Ex. J.)

Throughout this process, the United States made productions of materials from Twitter and Discord to Defendants in discovery. Initially, these productions were co-extensive with the information the United States seized for its Case File under the Social Media Warrants. In May 2023, however, counsel for Defendant Hennessey repeatedly requested that the United States produce all social media messages of Defendant Hennessey, beyond what had been seized as part of the Case File Return and already produced. In response to this repeated discovery request, the United States produced to all Defendants (to maintain discovery parity) all Twitter messages and Discord channel exchanges disclosed by Twitter and Discord, regardless of whether they had been reviewed or seized for the case file (the "Additional Warrant Material").

In its production letter to Defendants, the United States expressly disclaimed any intent to use the Additional Warrant Material in its case-in-chief, and made clear that the United States had *not* seized the Additional Warrant Material as part of the search warrant review, but was producing the Material in good-faith response to Defendant Hennessey's repeated requests. (*See* ECF No. 451, Ex. K at 2–3.) The production letter stated:

> Please note that the above-referenced Discord and Twitter materials are being produced solely at the request of counsel for Defendant Hennessey and in an abundance of caution. We do not believe that this information is relevant and material to the defense; the material is also beyond the scope of what we seized as part of the search warrant and maintained in our case file. We have no intention to use in our case in chief any materials from Discord or Twitter that was not previously produced to you.

(*Id.* at 3.)

To facilitate Defendants' review of the Additional Warrant Material—which the United States had *not* reviewed for substance and *not* added to its files—the United States provided data

to Defendants in a searchable and sortable format, in addition to the original versions.[2] Mr. Varani processed certain of this data by running Python scripts (automated processes) to convert the largely unreadable text files to other formats, like Microsoft Excel similar to the readable, "processed" files in the Case File Return. In so doing, Mr. Varani did not substantively review the contents of the data for relevancy purposes under the Social-Media Warrants.

III. Defendants' Motion presents a series of arguments that are self-refuting when applied to the actual facts and law.

Defendants make three principle complaints, which they assert somehow (without basis in law) constitute grounds for suppression of *all* records from Twitter and Discord. Namely, that the United States:

1. stored an intact and segregated original copy of the data disclosed by Twitter and Discord, including data that is not relevant to the charges against Defendants;
2. produced this complete copy—at the request of Defendant Hennessey—to the Defendants; and
3. contacted Twitter in the months following the execution of the Twitter Warrant to rectify Twitter's seemingly inadvertent error in omitting in Twitter's original production information within the scope of the warrants.

None of these points merit relief, let alone the relief Defendants seek.

The United States obtained lawful search warrants based on probable cause—which Defendants *do not dispute*—and executed them according to their terms. The procedure the United States followed in obtaining and reviewing the data accords with the statute under which the

[2] Defendants' oft-repeated argument about time-stamp issues arising from initial processing with the Axiom tool is another utterly irrelevant attempt to muddy the record. To the extent Defendants are concerned that any data processing affected time stamps, the United States *provided the original underlying records* as well, so Defendants have the *complete ability to confirm the integrity of each and every time stamp* they so desire. Defendants can confirm the time stamp accuracy of the United States' trial exhibits with the underlying original records. And the United States will not be using at trial any files processed by the Axiom tool, so this is not an issue in this case despite Defendants' attempt to manufacture one.

electronic search warrants were issued, 18 U.S.C. § 2703; the Federal Rules of Criminal Procedure; and applicable case law—as well as with the Fourth Amendment. The United States has taken steps to make sure that the information ordered for disclosure by the Court is diligently received, reviewed, and retained. Even if there was a technical violation (there was not) the remedy is not suppression of all returns from Twitter and Discord, as Defendants cite no prejudice, and the United States has acted in good faith within the language of the validly issued Warrants.

To the extent Defendants complain about the production—of the Defendants' own unreviewed materials to Defendants themselves—of materials outside the scope of what was seized by the United States, they should lodge their complaints with Defendant Hennessey and his *request for those materials*, not with the United States.[3] Defendants' silence as to *why* the United States produced to them materials from the Social-Media Warrants beyond the Case File Return speaks volumes.

Further, the United States has consistently disclaimed reliance on the Additional Warrant Material. So even if the out-of-scope information were suppressed, there would be no practical impact at trial. "Blanket suppression" of all material from Twitter and Discord, including the Case File Returns that were validly compiled under the warrants' specifications, is disfavored under the law, illogical, and entirely inappropriate here. For these reasons and those laid out below, the Motion should be denied.

[3] Each Defendant has standing with respect only to his own Twitter and Discord accounts. In the context of the search of an internet service provider account, a defendant does not have standing in an account that is not his own. *See, e.g.*, *United States v. Johnson*, No. 6:14-CR-00482-MC, 2018 WL 934606, at *1–2 (D. Or. Feb. 16, 2018); *United States v. McGuire*, No. 216CR00046GMNPAL, 2018 WL 709961, at *2 (D. Nev. Feb. 2, 2018).

A. The Social Media Warrants were validly issued and executed.

Defendants do not argue that the affidavits supporting the Social Media Warrants fail to establish probable cause to search and seize records from Twitter and Discord. Nor could they. The affidavits lay out at length and in extensive detail how Defendants used Twitter and Discord to further their fraud. (*See* ECF No. 451, Ex. E at 12–35 (explaining probable cause), Ex. F at 12–39 (same)). Instead, Defendants assert that the seizure of information from Twitter and Discord constituted a "general search," but vacillate between objecting to the terms of the (validly issued) search warrants and complaining that the terms were not followed. Both tacks fail.

The Social-Media Warrants expressly authorized the United States' actions. The United States applied for and received warrants that instructed Twitter and Discord to disclose sets of information. The warrants further authorized the United States to conduct "a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in [the] warrant." (ECF No. 451, Ex. E at 52, Ex. F at 49.) Attachment B of the Social Media Warrants explicitly provided that "the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review." (*Id.*, Ex. E at 53, Ex. F at 50.) The United States complied with these instructions, as issued by the Magistrate Judges.

Even setting aside the language of the Social-Media Warrants, the Federal Rules of Criminal Procedure, the Stored Communications Act, and applicable case law all approve of the United States' approach to its execution of the Warrants.

1. The United States followed the two-step review procedure from Rule 41.

The "two-step" procedure for the collection and review of electronically stored information (ESI) under a search warrant, which Defendants submit has caused "discomfort" in some out-of-

circuit district courts, is built into Rule 41(e)(2)(B). That Rule provides for "a later review of the media or information" following "the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). In its comments to the 2009 amendments to Rule 41 that added this language, the Advisory Committee expressly explained, due to the large amounts of information contained in electronic media, "the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41, Advisory Committee's Notes (2009 amend.). The Advisory Committee noted that a judge *may* set a deadline for the return of the storage media but *chose not* to impose such a requirement. *Id.* Indeed, the Fifth Circuit has recognized that the Fourth Amendment itself "contains no requirements about when the search or seizure is to occur or the *duration*." *United States v. Jarman*, 847 F.3d 259, 266 (5th Cir. 2017) (cleaned up).

Notably, the Magistrate Judges in this case did not set such a deadline or requirement regarding non-responsive information. This Court has no basis to suppress evidence seized and retained within the parameters of the search warrants duly issued by the Magistrates Judges in accord with all applicable law, even if other judges have opted—at the time the warrant is issued—to require that the government return or delete such records, a condition notably absent here. *See, e.g.*, *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (requiring the United States to return irrelevant records to a cell phone provider where they implicated the privacy interests of hundreds of third parties). Defendants' policy objections to the Federal Rules of Criminal Procedure and the practices of the Magistrate Judges in this case do not entitle them to "blanket suppression" of lawfully obtained evidence.

There are also reasonable considerations contrary to Defendants' irrelevant policy preferences. The Second Circuit, for example, in *United States v. Ganias*, 824 F.3d 199, 215 (2d Cir. 2016) (en banc), explained several reasons why the retention of a complete data set may be important. For instance, "[p]reservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial," and "may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved." *Id.* In *Ganias*, the defendant challenged the government's retention and successive search of hard drives containing both responsive and non-responsive data. *Id.* at 200. Although the *Ganias* Court upheld the Government's actions on the basis of good faith and so did not issue a holding on the Fourth Amendment retention question, *id.* at 225–26, its reasoning was prescient: in this case, at least one defendant actually *has* requested the full set of messages received as part of the Social Media Warrants. Based on this request, the United States produced to all Defendants (to maintain discovery parity) the information disclosed by Twitter and Discord, which went beyond what the United States had reviewed or seized for its case.

Defendants cannot have it both ways. If they want all data disclosed to the United States by Twitter and Discord, they cannot then use the United States' good faith response to that request to attack the United States' production of that data, or the wholly separate and legally sound Case File Return. Had the United States deleted the non-responsive data after running its search terms and seizing the relevant information for its case file, Defendant Hennessey (and likely others) would surely complain about the spoliation of evidence and would argue speculatively about the

value of the deleted records.[4] Instead, the United States chose to take the cautious approach by maintaining and, subsequently, in response to Defendant's request producing the Additional Warrant Material to Defendants so that they may conduct their own review and evaluation.

This is not to suggest that Defendants must reciprocally allow the United States to substantively review the full set of information disclosed by Twitter and Discord, which extends beyond the scope of the warrants. Rather, the appropriate process is what the United States has done in this case: seize relevant information for its case file and maintain a separate copy—with the balance of the records unreviewed—which Defendants may request in discovery. It bears repeating that the United States has not used and will not use at trial any information outside the scope of what it set out to seize in the second step of Attachment B and has maintained as the Case File Return. Defendants can confirm (and should have confirmed before filing) this fact by comparing the United States' trial exhibits with the Case File Return.

In fact, the United States has taken significant steps to limit its review of the information disclosed by Twitter and Discord to the scope set forth in the second "step" of Attachment B. Specifically, the United States has employed particular search terms to identify relevant records within the universe of the private personal information disclosed by Twitter and Discord. Only records responsive to the search terms, along with certain subscriber data and metadata, and publicly posted content, have been added to the Case File Return. This approach has been taken in an abundance of caution. Courts have hesitated to require even this much, recognizing that "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes." *United States v. Ulbricht*, 858 F.3d 71, 102

[4] To be clear, the United States has no basis to believe that the Additional Warrant Material contains exculpatory information.

(2d Cir. 2017), *overruled on other grounds by Carpenter v. United States*, 138 S. Ct. 2206 (2018); *see also Andresen v. Maryland*, 427 U.S. 463, 482 (1976) ("[I]t is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

2. Twitter's delayed disclosure of certain information ordered by the warrant should not result in suppression.

The Twitter Warrant issued by the Magistrate Judge ordered Twitter to produce certain records, including IP data and multimedia associated with Tweets and messages. (*See* ECF No. 451, Ex. E, at 49–50 ("All . . . subscriber information, . . . including . . . Internet Protocol ('IP') addresses . . . ."; "All content . . . relating to communications . . . including all attachments, multimedia . . . .").) But Twitter's initial production in response to the execution of the Twitter Warrant inadvertently omitted some of this information.

The United States promptly contacted Twitter once this inadvertent omission was realized and Twitter produced the records called for by the Twitter Warrant. At no point did the United States "go back to the well" for records outside the scope of the initial warrant. This is demonstrated by the fact that Twitter referenced the initial Twitter Warrant as the basis for its production and did not require further legal process to address the omission and produce the materials. (*See* ECF No. 451, Ex. J.) This straightforward resolution of an error on the part of a third-party provider should not be held against the United States.

i. The warrants were executed when they were timely served on Twitter.

The United States executed the Twitter Warrant when it served it on Twitter—within 14 days of its issuance. The affidavit on the basis of which the Twitter Warrant was issued specifies that "the government will execute this warrant by serving the warrant on Twitter." (ECF No. 451, Ex. E at 45.) Defendants' argument to the contrary is based on a misunderstanding of the law. They

assert that "the government had 14 days to seize the electronically stored information from Twitter," ECF No. 451 at 17, after which the warrant expired—and so any information received after that date would be outside the warrant. This argument rests on a sentence in a subsection of Rule 41, which states that the time for execution under the rule is the time the media is seized on-site, not the time the media is later copied or reviewed off-site. Fed. R. Crim. P. 41(e)(2)(B).

But this timing provision, which was developed for traditional, physical search warrants, bears differently on warrants under the Stored Communications Act, 18 U.S.C. § 2703, which governs remote, electronic searches, like the ones in this case. *Compare* Rule 41(e)(2)(A) *with* Rule 41(e)(2)(B). Warrants under the Stored Communications Act are different than traditional, physical search warrants. They do not adopt all the provisions of Rule 41 of the Federal Rules of Criminal Procedure, which makes sense given the different context of electronic media searches. *See, e.g.*, *United States v. Ackies*, 918 F.3d 190, 200 (1st Cir. 2019); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008).

Notably, Congress included 18 U.S.C. § 2703(g), which specifies that "the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service." This provision indicates that the execution of an SCA warrant begins when the officer serves the warrant on the service provider.

Courts to have addressed this question have held that a warrant under the SCA is "executed" on the date that it is served on the service provider. *United States v. Farrad*, 895 F.3d 859, 890 & n.23 (6th Cir. 2018); *United States v. Allen*, 2018 WL 1726349, at *8 (D. Kan. 2018); *see also United States v. Haile*, No. 2:22-CR-20629, 2023 WL 4118568, at *5–6 (E.D. Mich. June

22, 2023) (citing *Farrad* and *Allen*). In these cases, the agents served warrants on third-party providers within fourteen days, but the providers did not provide information in response to the warrants until after the fourteen-day period. *See Farrad*, 895 F.3d at 890; *Allen*, 2018 WL 1726349 at *8. In both cases, the courts found that the fact that the providers did not provide information within the fourteen days did not change the analysis—the warrants were timely "executed" when the agents served them. *Farrad*, 895 F.3d at 890; *Allen*, 2018 WL 1726349 at *8. This Court should follow the courts to directly address this issue[5] and find that the date of execution is the date on which the agents served Twitter with the warrants.

ii. A rule of suppression of all records produced outside the 14-day window is unworkable and illogical.

To award Defendants a legally unsupported windfall in the form of the "blanket suppression" of unrelated relevant evidence to punish a third-party omission unconnected to the United States' actions would create a nonsensical new remedy that affronts justice. This remedy is inconsistent with the aim of the exclusionary rule: to deter illegal searches and seizures by the government. *Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 362–63 (1998).

Practically, this rule is unworkable and illogical because it would put a significant burden on third parties to comply with warrants, and/or penalize the United States for the third parties'

[5] One court has contemplated that the date of "execution" could be the date on which the provider discloses the information. *United States v. Nyah*, 928 F.3d 694, 699 (8th Cir. 2019). In *Nyah*, the Eighth Circuit stated in *dicta* that "the text of Rule 41 suggests that a warrant is not fully executed until officers have seized the property that they are authorized to take" and "the authorized seizure of property under the warrant constitutes part of the execution of the warrant." *Id.* The *Nyah* Court, however, made clear that it was merely "raising questions" about the issue and not issuing a holding or "unnecessarily creating a conflict in the circuits on sparse briefing." *Id.* at 700 n.3. And a concurrence in part by Judge Stras criticized the majority for even addressing this issue in *dicta*. *Id.* at 701 (Stras, J., concurring in part) ("The court says more than it needs to about an issue that it never decides: whether a warrant is "executed" when it is delivered to someone in possession of digital data or, instead, when the data is finally turned over to the authorities."). This Court should avoid further muddying the opinions on this issue follow the sensible approach taken by courts that have actually decided the question.

failure to do so. The Stored Communications Act, however, does not enlist third parties to ensure that warrants are timely executed. The plain language of the statute only allows the United States to "require the disclosure by a provider of electronic communication service" of information pursuant to a warrant. 18 U.S.C. § 2703(a). The SCA does not allow the United States to order a third party to provide the information within fourteen days of the execution of the warrant. *Id.* Nor can the United States, as a practical or legal matter, send an agent to ensure that all in-scope data is provided within 14 days. *See* 18 U.S.C. § 2703(g) (allowing agents to serve warrants remotely). Defendants' policy proposal is simply at odds with law, logic, and the purposes and realities of remote electronic searches.

iii. Violations of Rule 41's timing requirements do not require suppression.

Even if Defendants could somehow establish that Twitter's failure to timely produce multimedia attachments and IP address data was the fault of the United States (they cannot), the fault would be at most a technical violation of Rule 41's 14-day period for seizing or copying electronic information (it is not).

The Fifth Circuit explained that "a violation of the rule governing the execution and service of a search warrant is 'essentially ministerial in nature and a motion to suppress should be granted only when the defendant demonstrates legal prejudice or that non-compliance with the rule was intentional or in bad faith.'" *United States v. Jacobs*, 125 F. App'x 518, 522 (5th Cir. 2005) (unpublished) (quoting *United States v. Marx*, 635 F.2d 436, 441 (5th Cir. 1981)); *accord United States v. Beckmann*, 786 F.3d 672, 680 (8th Cir. 2015) ("When the government violates Rule 41, the Court may exclude the evidence described in the search warrant only if the defendant is prejudiced or if reckless disregard of proper procedure is evident.") (cleaned up), *United States v.*

Williamson, 439 F.3d 1125, 1132 (9th Cir. 2006) ("[S]uppression is rarely the proper remedy for a Rule 41 violation.").

Defendants point to nothing approaching this demanding threshold. They have suffered no prejudice, and do not attempt to argue otherwise—the word "prejudice" does not appear in their Motion. And Defendants' attempt to malign the United States' good-faith efforts are belied by the facts. The Twitter Warrant ordered Twitter to produce certain information, and Twitter produced it. Defendants have identified no information disclosed by Twitter that falls outside the scope of what Twitter was originally directed to disclose under a validly issued search warrant. Nor does the United States' outreach to Twitter imply bad faith or recklessness—indeed, it reflects the opposite, due diligence—as the United States promptly served the Warrant on Twitter when it was issued, did not unreasonably delay the execution, and addressed a seemingly inadvertent omission as soon as it was discovered. As noted, the United States' production of materials outside its own case file does not imply that the United States has reviewed these materials or intends to use them at trial.

B. There is no basis in law or fact for "blanket suppression" of the Social Media Warrants because the United States acted in good faith and will not use material beyond the scope of the Warrants

Defendants cannot show any violation, constitutional or statutory, but if they could, they would still not be entitled to the drastic relief they seek: the "blanket suppression" of all evidence obtained under the Social Media Warrants. (ECF No. 451 at 23.) First, the United States acted in good faith on the basis of lawfully issued warrants as already described. Second, even if suppression were an appropriate remedy, that suppression would be limited to materials *outside* the scope of the warrant—materials on which the United States has already *disclaimed* reliance at trial or otherwise, rendering moot any remedy to which Defendants could possibly be entitled.

1. The United States acted in good faith.

The Court need not even reach the Fourth Amendment question because the record reflects that the United States acted in good faith on the basis of the warrant, which renders suppression inapt. *See, e.g.*, *United States v. Pawlak*, 935 F.3d 337, 346–47 (5th Cir. 2019) ("'[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.'" (quoting *United States v. Leon*, 468 U.S. 897, 922 (1984)).

The Fifth Circuit has articulated four circumstances in which the good-faith exception to the exclusionary rule may not apply:

> 1. When the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false;
> 2. When the issuing magistrate wholly abandoned his judicial role;
> 3. When the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and
> 4. When the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers cannot reasonably presume it to be valid.

United States v. Beverly, 943 F.3d 225, 232–33 (5th Cir. 2019) (citation omitted). Defendants do not articulate how any of these circumstances apply in this case, because none of them do. And, as discussed, Defendants do not dispute the existence of probable cause. This should be dispositive.

Defendants' attempt to circumvent good faith by arguing that the United States "did not properly execute the Warrants in accordance with their limitations," ECF No. 451 at 25, is belied by the record already described. Defendants may disagree with the scope of the Warrants and their provisions, but they cannot reasonably claim that the United States ignored them.

2. The United States will not use out-of-scope material at trial.

Even assuming an action had been unreasonable and not redeemed by good faith reliance (which is not the case), there would still be no basis to suppress records that fall unquestionably

within the scope of the Social Media Warrants. And those in-scope records are all that the United States ever planned to use at trial. Suppression of other records from the Social Media Warrants, even if called for here (it is not), would be a remedy without application because nothing that would be suppressed is being offered as evidence. The Motion is moot on arrival. This fact alone lays bare Defendants' Motion for what it is: a desperate attempt to preclude lawful evidence Defendants have no legitimate way of countering under fact or law.

Put simply, if Defendants are concerned that the United States has access to materials outside the scope of the Warrants, the appropriate remedy is suppression of the materials *outside the scope of the Warrants*.[6] But the United States has already committed that it will not use these materials. Defendants *can confirm* this fact by comparing the United States' trial exhibits to the Case File Return.

The Motion asserts that blanket suppression is necessary to deter the United States from disregarding the Warrants' limits, but this is based on—at best—a misunderstanding. The United States has not, and will not, casually peruse the information disclosed by Twitter and Discord. As noted, the United States has confined its review to the scope of the second step of Attachment B by running targeted searches and seizing only the relevant results in the Case File Return. There is nothing to deter. If Defendants doubted this, they could have asked the United States prior to filing the Motion, as required by the Court's Rules and as they consistently fail to do. *See* J. Hanen, Criminal Procedures 6(A).

[6] As a scholar has observed, "it would be harsh medicine indeed if a warrant issued on probable cause and particularly describing certain items were to be invalidated in toto merely because the affiant and magistrate erred in seeking and permitting a search for other items as well." § 4.6(f) Partial invalidity, 2 Search & Seizure § 4.6(f) (6th ed.).

In a sense, Defendants and the United States agree: information outside the scope of step two of Attachment B to the Social Media Warrants should not be used by the United States at trial. The only potentially appropriate remedy here (which doesn't apply) would result in what is already the status quo—precluding what will not be offered—rendering the Motion moot.

3. There is no basis for blanket suppression, and the only Fifth Circuit case Defendants cite supports the opposite conclusion.

Defendants have offered no legal or factual basis for their extreme requested relief.[7] In the only Fifth Circuit case Defendants cite for the proposition that blanket suppression is warranted, *United States v. Kimbrough*, 69 F.3d 723 (5th Cir. 1995), the court rejected defendant's request for blanket suppression. In *Kimbrough*, the defendant challenged a premises search warrant as "general" when it the officers seized "virtually every record." *Id.* at 728. But the court rejected the argument because items shown not to be relevant after an "initial review" were left behind, and because the defendant could cite no support for the absence of good faith. *Id.* To the extent that the premises search warrant in *Kimbrough* is analogous to the electronic search warrants in this case, *Kimbrough* supports denial of the Motion.

IV. Conclusion

For the foregoing reasons, the Motion should be denied in its entirety.

[7] Indeed, there exists significant authority to the contrary. *See, e.g.*, *Davis v. United States*, 564 U.S. 229, 237 (2011) ("Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." (citations omitted)).

Dated: November 1, 2023

Respectfully submitted,

GLENN S. LEON
Chief, Fraud Section
Criminal Division, Department of Justice

By: */s/ John J. Liolos*
Scott Armstrong, Assistant Chief
John J. Liolos, Trial Attorney
Fraud Section, Criminal Division
United States Department of Justice
1400 New York Ave. NW
Washington, DC 20005
Tel.: (202) 768-2246

ALAMDAR S. HAMDANI
United States Attorney
Southern District of Texas

By: */s/ Thomas Carter*
Thomas H. Carter
Assistant United States Attorney
State Bar No.: TX24048387
1000 Louisiana Street, 25th Floor
Houston, Texas 77002
Tel.: (713) 567-9470

CERTIFICATE OF SERVICE

I hereby certify that on November 1, 2023, I will cause the foregoing brief to be electronically filed with the Clerk of the Court using the CM/ECF system, which will provide copies to counsel for all parties.

/s/ John J. Liolos
John J. Liolos, Trial Attorney
U.S. Department of Justice
Criminal Division, Fraud Section